



Contents lists available at ScienceDirect

Government Information Quarterly

journal homepage: www.elsevier.com/locate/govinf

Key issues in data center security: An investigation of government audit reports

Kenneth J. Knapp^{a,*}, Gary D. Denney^b, Mark E. Barner^c^a John H. Sykes College of Business, The University of Tampa, 401 W. Kennedy Blvd. Tampa, FL 33606-1490, USA^b Department of Management, HQ USAFA/DFM, 2354 Fairchild Drive, Suite 6H-130, USAF Academy, CO 80840-5099, USA^c WIC Program, Mountain Plains Region, United States Department of Agriculture, Denver, Colorado 80246-1530, USA

ARTICLE INFO

Available online xxxx

Keywords:

Data center
Information security
Audit reports
Common body of knowledge
Operations security
Physical security
Disaster preparedness

ABSTRACT

The rising volume of electronic data, the growth in cloud computing and the need for secure and affordable large-scale data storage all contribute to the increasing reliance on data centers in society. This paper provides an overview of security issues relevant to data centers. We offer an aggregation and exploratory analysis of four audit reports of government data centers operating in the United States. Using the information security common body of knowledge to categorize audit findings, we identify the key issues from the reoccurring findings in the reports, particularly in regards to operations security, data center management, physical security, and disaster planning. The security of data centers has become a paramount concern for both government and the information technology industry. Both practitioners and academics can benefit from our research results because it provides insight into the key security issues facing modern data centers.

© 2011 Elsevier Inc. All rights reserved.

1. Introduction

In a style reminiscent of the 'wild west' days of the nineteenth-century United States, two masked men allegedly pistol-whipped a lone IT staff worker during a graveyard shift, held the worker hostage for 2 h while confiscating equipment in a Chicago data center (Thibodeau, 2008). The burglars reportedly entered the facility through a fire escape and passed an unoccupied security guard post. The thieves waited in hiding for the IT staffer to leave the data center and then ambushed and subdued the victim. The thieves swiped the staffer's access card through a reader and forced him to perform a finger print scan before stealing computer storage equipment. Since the incident, the company has hired armed guards to patrol the data center and its perimeter. Today, organizations must protect data centers much like banks. Banks utilize many forms of security to include surveillance cameras, armed guards, panic buttons and inner sanctums or vaults to protect the most valuable bank treasures. The bank analogy is sensible considering modern society is in a digital age where information is a principal source of wealth and power. If this analogy is valid, then the larger data centers need protection much like the U.S. Bullion Depository at Fort Knox, Kentucky.

Data centers need protection not just from malicious human threats such as the Chicago incident described above, but also from human mistakes and natural disasters. A data center located in a flood zone faces obvious risks. However, floods can also occur in unexpected ways. In one instance, a Texas data center supporting mission critical

applications, including a criminal justice system, experienced an outage when a 90 year-old water main broke filling a basement with 6 ft of water. The basement contained vital electrical systems that supported a fifth floor data center. The flood resulted in a three-day electrical outage for the center forcing clients to use manual processing. Incidentally, two years prior to this event, an audit recommended that the organization develop a backup to the main center to better ensure business continuity in the event of an outage (Miller, 2010); unfortunately, the recommendation was never accomplished by the organization.

A data center is a central repository for the storage, management, and dissemination of data supporting one or multiple organizations. Every organization with computers has some type of electronic data center and every organization faces threats to their center. Smaller organizations may have their 'data center' stored on a single laptop or on a portable hard drive. Larger organizations may refer to a data center as a server room, server farm, computer room or a network operations center. Other organizations may have an internet data center, storage area network, or network attached storage structures. Organizations both large and small may store their data using cloud computing models where machines in large data centers can be provisioned in various ways to deliver services in a scalable manner (Wyld, 2009). The largest organizations often have multiple data centers located in different geographic regions and even across multiple continents to help mitigate risk in the event of a disaster at a single location. The above mentioned data storage configurations represent different types of data centers where the major difference is the magnitude or capacity of the center.

Yet, it is not enough to say that centers with sufficient storage capacity are necessary — data centers must provide *secure* storage. Despite the fact that cyber security gets more attention in the digital

* Corresponding author at: John H. Sykes College of Business, The University of Tampa, 401 W. Kennedy Blvd., Box O, Tampa, FL 33606-1490, USA. Fax: +1 813 258 7408.

E-mail addresses: kknapp@ut.edu, knappkj@gmail.com (K.J. Knapp).

age, breaches seem to continue unabated. One non-profit organization estimates that there has been more than 350 million records containing sensitive information involved in security breaches in the U.S. between 2005 and 2010 (Privacy Rights Clearinghouse, 2010). Surprisingly, nearly half of the breaches were not the work of devious network hacks, but direct data storage losses, such as the 2006 U.S. Veterans Administration loss of storage devices containing records on millions of patients. At the same time, we are seeing rising amounts of sensitive electronic data from financial transactions, electronic health records and security sensors. Organizations today need efficient and affordable data storage facilities that are also secure, reliable and available.

If we need secure data centers, how should we design them to maximize protection from various security threats? The notion of defense-in-depth is one approach stipulating multi-leveled security where processes penetrate deep into an organization; it suggests layers of security offering both redundancy and diversity to protect from threats. Defense-in-depth is receiving greater acceptance as a model for IT security and has been applied to the design of modern data centers (Santos, 2007). Practically, when building a data center facility, architects must design defense-in-depth considerations into the security philosophy of the structure. In one data center project, Terremark Worldwide constructed a 50,000-square foot facility using a tiered approach. For its most sensitive systems, there are seven layers of physical security before a person can even touch a computer. These layers consist of a variety of security devices to include biometrics, gates, fences, guards, identity cards, and even ditches and hills. Some of the fencing is rated strong enough to stop a truck moving at 35 miles per hour (Hoover, 2008). Another organization anonymously reported building what seemed to be a simple retention wall three feet high around its data center. In reality, the wall extended nine feet underground with steel reinforcement built to withstand a 60 mile per hour hit from an 18-wheel truck loaded with explosives. Other organizations, such as Deutsche Bank and Continental Airlines operate data centers and backup facilities in highly protected underground bunkers often as deep as 60 feet below the surface (Mitchell, 2009). The U.S. National Security Agency is building a massive, \$1.7 billion, one million square foot data center in Utah as a self-contained complex with its own water supply, sewer system, power backups and anti-terrorism defenses (Omaha World Herald, 2010).

An objective of this paper is to provide an overview of key issues facing data centers drawn from investigating publically available audit reports. We offer an exploratory analysis of data center audits that can form a baseline for a future confirmatory study on this pertinent topic. To our knowledge, no published academic study exists that aggregates results across multiple data center audits. In fact, we found very few studies on data centers at all in the published information systems scholarly literature. This is particularly important considering the growing reliance on cloud computing and data centers in both government and commercial information technology architectures (Paquette, Jaeger, & Wilson, 2010). Having introduced the topic, we now analyze four audit reports of government data centers located in the United States. We then summarize the reports and offer a discussion of the results. Before concluding, we provide our research contributions and study limitations.

2. Analysis: four data center audit cases

The authors analyzed four publicly available reports detailing the findings of data center audits. While individual audits vary in scope and goals, in general, audits help to ensure that a data center has adequate physical, operational, cyber, environmental and managerial controls in place to prevent harmful incidents and thus protect the data resource. Audits may also check for compliance with applicable laws, regulations or internal organizational policy. If professionally accomplished, audits highlight weaknesses and offer practical re-

medies to improve data center management, operation, and security. Analyzing audit reports can be valuable since they summarize the essential concerns and security challenges facing modern data centers. Next, we briefly provide a background of audit approaches and methodologies before analyzing the four specific cases.

2.1. Background

As an aide to the reader, we offer some background information about data center audits. To begin, it is important that competent specialists conduct data center audits. In addition to direct experience, professional certifications such as the broad-based Certified Information Systems Security Professional (CISSP) or the more audit-focused Certified Information Systems Auditor (CISA) add credentials to the auditor. Many audits are conducted in accordance with government standards such as those published in the United States by the General Accounting Office. In addition, auditors can reference applicable laws, organizational policies, and industry standards such as from the Information Systems Audit and Control Association (ISACA). Other helpful references include material from the IT Governance Institute, the IT Infrastructure Library (ITIL), the Telecommunications Industry Association (TIA) 942 document on data center standards as well as the Statement on Auditing Standards No. 70 (SAS 70) which provides direction on auditing service organizations to include data centers. Other professional resources are available from organizations such as the SANS Institute and IEEE.

Data collection for audits typically emanate from various sources. Here, we list six sources used in the audit cases of our study. First, auditors can assess security through observation to include site survey and facility tours. Second, auditors can talk to data center workers through formal interviews or from spot questions made during facility visits. Third, automated tools are available to test important network systems such as firewalls and access control systems. Fourth, auditors can review control records to include facility access logs and system accounts. Fifth, auditors may directly test (although often in a limited fashion) critical systems such as fire suppression or backup power systems. Sixth, auditors may review management documents such as disaster recovery plans, security training programs, support-level agreements or risk assessments.

Additionally, from reviewing the four audits, a general methodology for conducting an audit was apparent. While different data center audits have varying objectives and levels of scope, below we provide a general timeline over five phases:

1. *Schedule audit* can be scheduled more than 1 year in advance or can be an unannounced 'surprise' audit.
2. *Audit event* duration can last just a few hours or over several months.
3. *Report of findings* should be promptly issued after audit completion to data center management.
4. *Response* is given by management for each finding in the report and provides a planned solution to identified weaknesses.
5. *Progress and status report(s)* are provided by the data center as an update on implementing security fixes.

Once an audit begins and through its completion, we can divide audit climates into two types: cooperative and contentious. In our study, we have examples of both types. Yet, it seems that if the auditors are professional and respectful toward data center staff and the staff sincerely desires to improve overall security and operation of the center, there *should* be little reason for a contentious climate during an audit.

2.2. Case selection

Following are summaries of four data audits of government data centers. The first author accessed each report through the internet. We

selected each audit case so that a variety of government audits focusing on data center security issues could be included in our sample. Additionally, we considered only audits with clearly written findings that were applicable to our research goal of aggregating the findings. We used government audit reports considering that many are publically accessible, usually in accordance with jurisdictional laws. This could not be possible with audits of commercial organizations since no law would require it; indeed, publicly doing so is unexpected since audit reports commonly reveal security weaknesses. Moreover, we found it increasingly difficult to find data center audit reports focusing on security issues dated after 2007; we gather that many governments no longer mandate the posting of data center audits if they reveal security weaknesses or at least are delaying posting until after weaknesses are fixed. Given our criteria, after searching the .gov top-level domain, we found nine audit reports that met our research goals. We selected four security-focused reports which represent different levels in the government (federal, state, city) suitable for our research.

For each audit case, we provide a background and a summary of the findings. The first audit was conducted at the Internal Revenue Service in 1996 and offers a valuable historical perspective of a data center audit. The second was conducted in 2006 supporting a State of Montana data center. The third was a 2006 audit assessing a New York City Police Department data center. The fourth was a 2007 audit of a State of Michigan data center. We then classify each audit finding into one of the ten common body of knowledge (CBK) categories, which we will discuss further in Section 3.

2.3. Case #1: Internal Revenue Service

Our first case provides an historical example of a highly critical audit of an Internal Revenue Service (IRS) data center. The IRS is the United States government agency that collects taxes and enforces internal revenue laws for the Federal Government. As such, the IRS is a very information intensive organization that relies heavily on technology. On March 12, 1996, the United States General Accounting Office (GAO) conducted a review of an IRS data center. This data center was a \$17 million project (1996 dollars) supporting a new electronic filing system called Cyberfile. The GAO auditors understood that this data center was to go into production on March 19, 1996 and conducted the audit one week prior. The audit identified 49 weaknesses across seven categories including data center operations, physical security, data communications management, disaster recovery, contingency planning, risk analysis, and security awareness.

Of the 49 specific findings, some were temporary issues such as identifying the need to move combustible materials outside the data center. Other issues were structural such as noting that the data center is located on a subbasement level of a building without water detectors under the raised floor. Additionally, the audit noted the commingling of fiber optic lines in the same network switch from the IRS and another building occupant potentially exposing the lines to unauthorized access.

The IRS strongly protested the GAO audit report that listed many serious security weaknesses. First, the IRS contested that the operational date of March 19, 1996 as understood by the GAO was incorrect. In their reply to the GAO audit, the IRS stated that on March 1, 1996, 12 days prior to the GAO audit, the IRS executive committee and external partners were notified that the Cyberfile data center would not be in production as initially planned. Secondly, the IRS contested many of the findings as inherent to a non-production data center under construction, such as the first finding about large amounts of combustible material located inside the center. While the miscommunication between the GAO and the IRS was unfortunate, the IRS did acknowledge a number of potentially serious weaknesses. For example, regarding the lack of water detectors under the raised floor, the IRS developed a proposal for the deployment of such technology the month following the audit. The duration of the audit was actually cut short as stated in the report's cover

letter, "...because so many weaknesses were identified in about one hour, we did not continue with the in-depth review that we typically provide" (GAO, 1996).

The Cyberfile data center case provides a valuable and historical study in how a contentious data center audit can still deliver useful results. Although dated to 1996, the findings offer insights that are still relevant for today's data center. The Cyberfile review was a high visibility review; the GAO addressed the report to a U.S. Senator and the IRS received negative media attention because of the report. While it is unfair to apply production-level security to a developmental data center, in our analysis, a large number of the 49 findings were legitimate regardless of the production status. The IRS quickly responded to the GAO review by claiming to have corrected 32 of the 49 weaknesses within 6 weeks of the review with plans to correct the remaining weaknesses prior to full production. However, the security problems at the data center may have been predictive of additional problems with the Cyberfile system; 6 months after the GAO audit, the IRS scrapped the system altogether (Chandler, 1996). In our analysis, the 49 findings from the audit provide a worthwhile case on how *not* to build a data center. We believe the findings are comprehensive enough to serve as a checklist of problems to avoid in data center development.

2.4. Case #2: Montana Department of Administration

The second case involves a data center audit of the State of Montana's Department of Administration. This Montana data center supports state agencies and stores data relating to accounting, budgeting, human resources, revenue, and public health and human services. The estimated total value of the data center equipment was \$14 million (2006 dollars). The focus of the audit was on the management and protection of the data center against physical, logical, and environmental threats. The scope of the audit included the entire data center and all of the resources within it, but excluded access controls related to any particular information system and network devices such as firewalls (Seacat, 2006; Stout, 2007).

The audit methodology included interviews with agency personnel, walkthroughs and inspections of the facilities, observations, and reviews of documentation and equipment configurations. The auditors referred to ISACA's Objectives for Information Technology and Control Practices, the Federal Information Systems Control and Audit Manual, as well as statewide IT policies. Overall, the auditors criticized the Department of Administration for not having processes to ensure operations continuity and for the lack of managerial controls that appropriately address data center threats.

The Montana audit report stated that data center management focused on providing operational services to other agencies. However, since the center stores some of the most sensitive data in state government (e.g. revenue related) the operational focus should side toward security. Additionally, the auditors found that multiple agencies were responsible for different aspects of security. For example, one agency was responsible for network security and another for physical security. The report stated, "The overlapping areas of responsibility created barriers to security efforts due to conflicting priorities. The department does not have somebody responsible for the data center as a whole, and for coordinating efforts to ensure security of the data center" (Seacat, 2006, p.14). The fifteenth recommendation in the report points this out and recommends giving a single entity responsibility for data center security as a whole.

The audit report contained fifteen specific recommendations for security improvement. In their response to the audit, while recognizing the seriousness of many findings, the Department of Administration concurred with all fifteen recommendations and assigned completion dates for fixing deficiencies. Although not as grave as the IRS audit, the Montana data center findings were nevertheless critical of the state of security. Also in contrast to the IRS case, the overall tone of the audit process from both sides appeared constructive and appreciative. A year

after the June 2006 report, the auditor released a memorandum that detailed progress made toward fixing deficiencies. However, a year after the June 2006 report, of the fifteen specific recommendations, only one was considered 'implemented' with thirteen considered 'partially implemented' and one 'not implemented' (Stout, 2007). In one finding for example, the audit report recommended to "conduct a cost analysis associated with implementing or improving controls." The Department's management concurred and stated that a "cost analysis will be conducted" based on a threat analysis with an estimated completion date of August 31, 2006. By June 2007, however, the department had only partially completed the recommendation.

2.5. Case #3: New York City Police Department

The comptroller of the City of New York, in accordance with a local city charter, conducted an audit of the New York Police Department's (NYPD) data center. The audit's focus was to ensure the center has adequate physical and computer system operations and that contingency plans are in compliance with Federal Information Processing Standards (FIPS) and City guidelines. The audit methodology was extensive, lasted 7 months in fieldwork duration and included interviews with NYPD personnel, surveys of the facility, reviewing pertinent policy documents and testing backup and recovery procedures (Thompson, 2006).

The audit concluded that the NYPD has adequate physical security and monitoring controls in place, sufficient security policies and a periodically tested disaster recovery plan. However, the report identified five control weaknesses. These include the lack of control of inactive user accounts, improper review and approval of an internet security plan, deficient testing of firewalls and content filters, an inadequate amount of emergency electrical backup power, and insufficient backup storage.

The NYPD response to the audit report was cordial and professional. The department agreed with four of the five specific findings and recommendations. By the time the NYPD released its formal response to the comptroller's office, some of the recommendations had already been implemented. The one finding the NYPD disagreed with regarded increasing the uninterruptable power supply (UPS) backup capability to provide additional time for manual activation of the generators in the event of an emergency. The audit team recommended providing more than the current 12 min of power. The NYPD argued that 12 min was more than adequate given that backup generators are designed to automatically engage in an outage. Even though the NYPD disagreed and did not implement the recommendation, the NYPD did install alarms that sound if UPS batteries are low or if the generators failed to engage during an outage. This countermeasure gave staff ample time to systematically power down data center systems if necessary. Thus, while the NYPD disagreed with the recommendation, they took a compensatory action to improve the situation.

As an afterword to the audit, a story of a significant "NYPD data center breach" occurred 3 years after the subject audit. Reportedly, an employee stole hardware containing personal information on 80,000 active and former NYPD police officers. The individual flashed an expired identification card to fool a security guard and gain access into the data warehouse (King, 2009). While the subject 2006 report did not reveal the location of the data center, it did seem to indicate that the NYPD had a single center at the time of the audit. Thus, it was interesting to read in the audit report that, "It is gratifying that the Comptroller found that the NYPD has adequate physical security controls that allow only authorized MIS Department staff and other approved NYPD personnel access to the Data Center" (Thompson, 2006, p. 14).

2.6. Case #4: Michigan Department of Information Technology

The final case of our study regards an audit of a Michigan data center operated by the state government's Department of Information

Technology. This center provides hosting for all State of Michigan agencies. The audit objective was to assess the effectiveness of efforts to protect the State's hosting centers from physical and environmental threats (McTavish, 2007). Like the first three cases of this study, the Michigan audit was security focused containing clearly written and suitable candidates for categorization of the findings into the common body of knowledge.

The audit scope included examining information processing and other records relating to data center operational control and was conducted in accordance with government auditing standards issued by the U.S. Comptroller General. The audit duration lasted 6 months starting in July 2006. Auditors used guidance from ISACA, the National Institute of Science and Technology (NIST) and the Information Systems Audit and Control Foundation (ISACF) which since has merged with the IT Governance Institute. The audit appeared to follow a high level of professionalism throughout in its conduct and comprehensiveness. The auditors not only pointed out noteworthy accomplishments but also clearly identified operational and security weaknesses. Five of the eight findings were outright security issues ranging from a lack of physical security controls at the server rooms to a lack of control with a vital telecommunications gateway. The remaining three findings were primarily directed at management but had secondary security considerations. For instance, the audit faulted management for not having an effective process of developing and maintaining service level agreements, which can cause problems regarding expected performance in the relationship between the data center and its clients. Overall, the audit report took a critical tone calling management "moderately effective" in administering the center.

The first finding and the most serious documented security weaknesses involved the lack of a comprehensive risk assessment. The department managing the center had failed to perform periodic risk assessments or reassessments when system or facility configurations changed. While the report recognized previous risk assessments, it criticized that they, "focused primarily on environmental controls, such as utilities, air conditioning, and fire suppression, as well as physical security controls. A more comprehensive risk assessment may consider the impact that natural disasters, neighboring hazards, hardware failures, internal procedures, a security program, and contingency planning could have on a facility's operation" (McTavish, 2007, p. 14). In another finding, the audit identified a material condition where the department failed to implement full security over the state's telecommunication gateway. The gateway provides a single point of access and data file transfer between business partners and one of the state's sensitive systems containing social security numbers, medical records and financial data. The finding comprised abundant criticisms including the failure to provide a full risk analysis of the gateway, to manage policies for governing gateway use and to monitor the activities of users with privilege gateway accounts. Overall, data center management largely agreed with the findings and said it would comply with the recommendations.

3. Categorization methods and results

The four audit reports documented 77 total findings. For categorizing the audit findings, we searched for a suitable framework that incorporates the broad range of security threats facing data centers and selected the information security common body of knowledge (CBK) for our study (Tipton, 2010). The International Information Systems Security Certification Consortium [(ISC)²] is a non-profit organization that manages the CBK and the CISSP program.¹ The CISSP is the first IT certification to be accredited under ISO/IEC 17024, a global benchmark for the certification of workers in various

¹ (ISC)², CISSP, and the *Common Body of Knowledge* (CBK) are registered marks. See www.isc2.org. In the literature, we have seen the CBK interchangeably referred to as the CISSP CBK, the (ISC)² CBK, and the information security CBK.

professions (Vijayan, 2004). This ISO certification adds credibility and validity to the (ISC)² organization as one of the world's foremost certifying bodies. Established in 1989, the CBK has provided a shared reference for information security professionals. Described on the (ISC)² web site, "the (ISC)² CBK is a taxonomy – a collection of topics relevant to information security professionals around the world... (it) establishes a common framework of information security terms and principles which allows information security professionals worldwide to discuss, debate, and resolve matters pertaining to the profession with a common understanding." Appendix A provides definitions of each CBK category (also called CBK domains in the security industry).

The authors selected the CBK model over other security models (e.g. the CIA triad) because of the CBK's comprehensive and practical orientation. Rather than being an academic framework, the CBK is inherently practitioner oriented and at a practical level for classifying real-world security issues facing data centers. During our analysis, we classified each of the 77 findings into one of the ten domains of the CBK. The first author initially classified each audit finding into one of the ten categories independently. Next, the two co-authors each independently reviewed and provided feedback to the first author on the classifications. After two rounds of review and discussion between the first author and co-authors, 100% agreement was reached on the categorization of the 77 findings. The CBK categorization process was moderately straightforward given that the audit reports themselves classified each finding into a category very similar, and sometimes identical, to the CBK. Appendix B contains a full listing of our categorization results.

We present two tables that summarize the aggregated findings of the four audit reports. Table 1 presents a numerical tally of the findings categorized by the CBK. Table 2 presents the same data except normalized as percentages instead of tallies. The percentage approach in Table 2 provides a standardized analysis of the findings thus removing the numerical bias primarily from the IRS audit, which included 49 of the total 77 findings. The percentages in the four columns for each case represent the percentage of findings for each CBK category for that particular case. For example, from Table 1, seven of the total 49 IRS findings were in the *access control* category; in Table 2, the seven findings equated to 14% of the 49 IRS findings in the same category. Also in Table 2, the mean percentage column represents the arithmetic mean of the percentages for all four cases. In both tables, we list the categories in ascending rank order, which differ between the tables.

4. Discussion

For analyzing our research results, we interpreted the table rankings as a key issues list in data center security. While each of

Table 2

Audit findings by percentages classified by CBK category.

Category	#1 IRS	#2 Montana	#3 NYPD	#4 Michigan	Mean percent	Rank
Governance and risk management	10%	33%	20%	38%	25%	1
Business cont. and disaster recovery	8%	20%	40%	13%	20%	2
Operations security	33%	0%	20%	13%	16%	3
Access control	14%	27%	0%	13%	13%	4
Physical and environmental security	18%	20%	0%	13%	13%	5
Telecomm. and network security	14%	0%	20%	13%	12%	6
Application security	2%	0%	0%	0%	1%	7
Security architecture	0%	0%	0%	0%	0%	8
Cryptography	0%	0%	0%	0%	0%	8
Legal, regulations, investigations	0%	0%	0%	0%	0%	8
Totals	100%	100%	100%	100%	100%	

the ten CBK categories can be critical in regards to data center security, the ranked results provide a list of what gets the most attention in data center audits, at least based on our sample. First off, it is clear that data center issues go well beyond what some may call 'traditional' computer security that includes concerns such as passwords, virus protection, denial-of-service attacks and network perimeter devices such as firewalls. Instead, data center security issues range in varying degrees across CBK topics. Based on the results in Table 1, the top three categories representing 58% of the findings include *operations security* (23%), *governance and risk management* (18%) and *physical security* (17%). Using Table 2, the top three categories representing 61% of the findings are *governance and risk management* (25%), *business continuity and disaster recovery planning* (20%) and *operations security* (16%). Although on neither top three lists, *telecommunication and network security* and *access control* also received substantial attention with each receiving findings in three of the four audit cases.

It is not surprising that *operations security* related findings topped the list in Table 1, considering the 16 IRS audit findings. Pertaining to data centers, operations security identifies the controls over the hardware, media, and the personnel who have access privileges to the center. It addresses the protection of data center assets while the data is resident in storage devices or in transit across networks in and out of the center. Some have argued that operations security is the heart of information security since it controls the way data is accessed and processed (Fisher, 2007). In data centers, operations security involves a broad range of critical issues. In the IRS report for example, operations security issues ranged from ensuring emergency cut-off switches are safeguarded from accidental cut-off or tampering to personnel safety concerns such as identifying that the facility needs emergency wash capabilities if workers are exposed to battery acid.

Governance and risk management was the top ranked category from Table 2. The category was one of two, with the other being *business continuity and disaster recovery planning*, that received at least one finding in each of the four reports. We could argue that every security finding is ultimately a risk management and governance responsibility to a certain degree. Still, a number of audit findings are solidly governance and management issues. In the Montana report, as previously discussed, the auditors recommended that the department clearly define responsibility for all aspects of security. This is a major finding because important responsibilities were divided among groups in different organizations creating "barriers to security efforts." Considering the importance of data centers today and the diverse threats they face, it's sensible to have a single organization or person responsible for security overall.

Three of the audit reports identified weaknesses in the *physical security* domain. The IRS report stated that the "data center did not

Table 1

Audit findings by numerical totals classified by CBK category.

Category	#1 IRS	#2 Montana	#3 NYPD	#4 Michigan	Count totals	Percent	Rank
Operations security	16	0	1	1	18	23%	1
Governance and risk management	5	5	1	3	14	18%	2
Physical and environmental security	9	3	0	1	13	17%	3
Access control	7	4	0	1	12	16%	4
Business cont. and disaster recovery	4	3	2	1	10	13%	5
Telecomm. and network security	7	0	1	1	9	12%	6
Application security	1	0	0	0	1	1%	7
Security architecture	0	0	0	0	0	0%	8
Cryptography	0	0	0	0	0	0%	8
Legal, regulations, investigations	0	0	0	0	0	0%	8
Totals	49	15	5	8	77	100%	

have a secure perimeter. Access to shared areas that completely encircle the data center was not controlled.” The Montana report identified similar problems. The data center, which was also in a shared building, did not have walls extended to the true ceiling and the office responsible for physical security was not aware of this vulnerability. With the Michigan report, auditors noticed a lack of policies governing physical security controls. These findings are worrisome considering that many data centers are in physically large facilities and taking into account threats such as the Chicago incident described earlier in this paper.

All of the cases had at least one finding related to *business continuity and disaster recovery planning*. This area is increasingly serious considering the role that data centers play supporting cloud computing and in light of disasters of the past decade (e.g. hurricane Katrina in 2005, terrorist events of 2001). As society in general moves more of its electronic data to internet-based cloud solutions, more data will as a result reside in large data centers. In the event of a disaster, whether natural or human-made, accidental or malicious, it is critical that data centers maintain reliable and available backup and recovery systems. Thus, the data center is responsible for maintaining a high-level of operational preparedness and continuity. If data is lost, a client may not have backups themselves if they are depending on the data center. Moreover, any data loss caused by a lack of diligence, planning or security increases the likelihood of lawsuits from clients. From the audit reports, we see the importance of this category in findings at the IRS, where auditors noted the lack of a backup computer facility and contingency plan, as well as at the NYPD, where auditors remarked about limited backup power. In the Montana report, auditors noticed a lack of statewide disaster planning and the Michigan report observed the lack of a developed and tested recovery plan.

From Table 2, 13% of the findings were in the *access control* category. This domain outlines various security options that control access to an organization's data processing resources. It builds on the concepts addressed in the information security governance and risk management category with an emphasis on administrative, physical, and logical controls (Hansche, Berti, & Hare, 2004). We took note that many physical security issues are logically access control issues as well, such as issues relating to security mechanisms along a center's exterior perimeter. Depending on the emphasis and wording of a particular audit finding, many physical and operations security findings had significant overlap with the access control category. We discuss this further in the *Research contributions and limitations* section.

Three of the four audit reports contained findings in the *telecommunication and network security* category. Considering that nearly all data moving in and out of data centers travel over telecommunication lines and that data centers internally utilize complex networking schemes, auditors must look at network security very carefully. Findings ranged from a lack of firewall testing at the NYPD data center to identifying exposed cable lines running along a ceiling exterior to the IRS data center. Additionally, the Michigan report emphasized a general lack of security with a critical data exchange gateway.

Three CBK categories did not have any classified findings: *cryptography*, *security architecture* and *legal, regulatory, compliance and investigation*. The *application security* domain contained a single finding from the IRS audit. However, it would be incorrect to conclude that these four categories are not relevant to data center security. Cryptography, for example, is essential when sensitive or confidential data travels in or out of a data center. Some laws, such as the U.S. Health Insurance Portability and Accountability Act of 1996, require certain types of sensitive data to be encrypted at least during transmission (HHS, 2008). Additionally, encrypting data “at rest” can be prudent especially if the data is extremely sensitive. Hence, assessing encryption may require dedicated audits with specialists knowledgeable in cryptography.

5. Research contributions and limitations

Based on our review of the literature, no prior study exists that aggregates findings across multiple data center audits. Thus, the contribution of this study is that it might be the first of its kind in the academic literature. Moreover, based on our review, this study is one of the few on data centers in the information systems academic literature. Additionally, much of the discussion of this study focused on operations and physical security, areas previously identified as lacking in the information systems literature (Knapp, Ford, Marshall, & Rainer, 2007). The CBK categorization framework allowed us to see the types of issues often identified as ‘findings’ enabling us to highlight the most critical areas in data center security. Our study can help practitioners and academics alike in obtaining an improved understanding of the security issues facing today's data centers.

Regarding research limitations, we consider our study exploratory since we analyzed only four audit cases in our sample. Thus, we cannot generalize our results or suggest that our study contains cases that are representative of typical data center audits. For example, some of the audits excluded certain areas of the CBK as in the Montana audit, where auditors considered computer applications and network devices to be outside of the audit scope. However, case study research with smaller sample sizes plays an important part in research contributions particularly as a reference for confirmatory, follow-on research with perhaps larger samples. An additional limitation is that our study used four historical audit reports as data sources. Thus, our approach did not explore the impact of some recent structural variations and trends in data center design, such as those regarding containerized data centers. Here, readers are encouraged to research trade publications to analyze how recent design innovations may affect data center security.

Our selected categorization approach has both strengths and limitations. As a strength, the information security CBK is a widely used industry framework and at the appropriate level for the categorization purposes of this study. In addition, the audit reports already categorized their findings using naming conventions similar to the CBK, making categorization somewhat straightforward. As a limitation, some of the findings overlapped CBK domains and could be classified in multiple categories. The most challenging categorization related to findings that overlapped the *access control* and *physical security* domains. For instance, we resolved many overlaps by placing access control related findings about the physical structure in the *physical security* category and access control related findings about administration and logic procedures in the *access control* category. Overall, we selected the closest single CBK category based on the writing emphasis of the audit finding.

6. Conclusion

In this paper, we provided an overview of security principles and key issues relevant to data centers. We then offered an exploratory analysis of four audit reports of government data centers in the United States before making general observations. This paper offers an investigative analysis of data center audits that can form a baseline for a future study on this relevant topic. Our results can help practitioners as well as academics in better discerning the key security issues facing the modern data center. Since data centers store large volumes of valuable and often sensitive information, proper security of data centers is essential. With the increased societal reliance on internet-based cloud computing for data storage and processing, the security of data centers has become a paramount concern for both government and the information technology industry.

Acknowledgment

An earlier version of this paper appeared in the *Proceedings of the Southern Association for Information Systems Conference*, Charleston, SC, USA, March 12th–14th, 2009.

Appendix A

Definitions of the ten common body of knowledge (CBK) domains based on Hansche et al. (2004) and Tipton (2010).

CBK domain (category)	Domain description
Access control (ACC)	Mechanisms that permit managers to exercise a directing or restraining influence over the behavior, use, and content of a system; outlines options that control access to information and data processing resources. Emphasis is on various administrative, physical, and technical/logical controls.
Application development security (APP)	Pertains to security concepts that apply during software development, operation, and maintenance processes.
Business continuity and disaster recovery planning (BCP)	The capability to process a critical business system in the event of disruption to normal business operations; the preservation of a business in the face of major disruptions.
Cryptography (CRP)	Addresses the principles, means, and methods of disguising information to ensure its integrity, confidentiality, and authenticity.
Information security governance and risk management (MGT)	The identification of information assets and life cycle management of policies, standards, procedures, and guidelines. Management tools such as awareness training and risk assessments are used to identify threats and implement security controls.
Legal, regulations, compliance and investigations (LEG)	Computer crime laws and regulations, investigative measures and techniques that can be used to determine if a crime has been committed.
Operations security (OPS)	Identifies the operational controls over hardware, media, and the operators and administrators with access privileges to these resources. The safeguarding of assets associated with the data processing environment.
Physical and environmental security (PHY)	The protection of information assets of an entire physical enterprise facility including people, data, equipment, systems, media and supplies.
Security architecture and design (ACH)	The concepts, principles, structures, and standards used to design, implement, monitor, and secure systems, equipment, networks, and applications. Used in controls that enforce various levels of availability, integrity, and confidentiality.
Telecommunications and network security (NET)	The structures, transmission methods, transport formats, and security measures used to provide protection of transmission over private and public communications networks and media.

Appendix B

Listing and categorization of audit findings. The first column indicates the finding category listed in the original audit report. The second column describes the audit finding and the third lists the CBK domain classified by the researchers of this study. All four cases are listed in this appendix: IRS, Montana, NYPD and Michigan data center audits.

Case #1: IRS Cyberfile data center audit results.

Audit category	Data center (DC) audit findings	CBK domain
Data center operations	1. Large amounts of combustible materials were found adjacent to and inside the DC.	1. OPS
	2. The DC's fire extinguishers required recharging and were haphazardly placed in the DC.	2. OPS
	3. The DC uses wet stand pipe sprinklers for fire suppression in lower than normal ceilings. Taller individuals have to duck to avoid hitting them which could inadvertently be damaged and release water.	3. OPS
	4. The DC is located on the subbasement level of a building and does not have water detectors under the raised floor.	4. OPS

Appendix B (continued)

Audit category	Data center (DC) audit findings	CBK domain
Physical security	5. Workstations had recordable drives that could be used to download taxpayer information or upload viruses.	5. OPS
	6. Emergency power cut-off switch not safeguarded against accidental cut-off or malicious tampering.	6. OPS
	7. Equipment racks were not grounded, increasing risk of electrical shock or fire.	7. OPS
	8. Smoke detectors in the ceiling were not activated.	8. OPS
	9. The DC had no plans for a secured magnetic tape library, increasing the risk of potential data loss.	9. OPS
	10. Backup batteries were to be installed in an unventilated room, increasing potential health hazard from toxic fumes.	10. OPS
	11. No wash facility available for individuals should they accidentally come in contact with battery acid.	11. OPS
	12. Air induction panels on the outside of the DC walls provided easy access to the DC by unauthorized individuals.	12. ACC
	13. Optical fiber lines from IRS and another building occupant were commingled in same switch, exposing IRS lines to unauthorized access.	13. NET
	14. Foam used to stabilize cables in the floor could create a toxic fire hazard.	14. OPS
	15. Cyberfiles' uninterruptible power supply was housed in the other occupant's area, exposing it to risk of tampering.	15. OPS
	16. The DC floor panels were open and electrical exposed, increasing the risk of injury to personnel.	16. OPS
	17. The DC equipment was operating while construction of the DC was taking place. The dusty environment placed the expensive and delicate computer and telecommunications equipment at risk of failure.	17. OPS
	18. The lock on the main door was improperly installed.	18. PHY
	19. Doors to the data center had unsecured hinges on the outside, allowing easy removal of the doors.	19. PHY
	20. Multiple exit doors were not alarmed or monitored by cameras.	20. PHY
	21. Packages and other articles were not inspected before being allowed in the DC, increasing internal security threats.	21. ACC
	22. Electronic card key devices installed on doors in an environment without guards or cameras do not limit access to authorized personnel only.	22. PHY
	23. Cigarettes were being smoked in the facility and smoke butts were in the piles of combustible materials.	23. PHY
	24. A large hole in the DC wall did not lead to the battery room, as DC personnel had stated. Instead, it leads to an area shared with the building's other occupant.	24. PHY
	25. Background investigations required for personnel working on secure facilities had not been conducted for personnel doing construction, pulling communications wires, and setting up DC operations.	25. ACC
	26. Background investigations required for personnel working on sensitive systems had not been conducted for personnel working on Cyberfile applications in the production environment.	26. ACC
	27. Personnel in the data center were not wearing any badges or other forms of identification to validate their authority to be in the data center.	27. ACC
	28. Vendors had unescorted access to the DC.	28. ACC
	29. Contractor personnel were developing and testing software in the production environment, not in a test facility.	29. APP
Data comm. mgt	30. The data center did not have a secure perimeter. Access to shared areas that completely encircle the data center was not controlled.	30. PHY
	31. Individuals entering the DC were asked to sign a log, but not required to show valid identification.	31. ACC
	32. Telecommunications equipment, such as switches, are not physically protected and could be accessed by unauthorized personnel.	32. PHY
	33. A communications device intended to be used only to monitor data flow could also be used for altering data and for browsing.	33. NET
	34. Communications lines were mounted unprotected on the back wall of the DC instead of being enclosed in a secure telephone closet or box.	34. NET

Appendix B (continued)

Audit category	Data center (DC) audit findings	CBK domain
Disaster recovery	35. No wiring plan for communications lines was available correlated the circuits with the wire locations.	35. MGT
	36. Communications lines from other facilities exposed the production environment to attack by outside individuals.	36. PHY
	37. Communications cables running along the ceiling outside the DC were exposed, providing a readily accessible target to be cut or wiretapped.	37. NET
	38. A separate communications line observed running through the DC posed an undetermined risk since DC personnel could not identify its origin, purpose.	38. NET
	39. Patch panels were installed at the DC, but no policies were established to control their use.	39. MGT
	40. A data communications block that was wired to route Cyberfile's electronic filing traffic was shared with traffic related to another application, increasing risk of communication disruptions.	40. NET
	41. Another data communications block that was wired to Cyberfile's public switch was also wired to route traffic for another application.	41. NET
	42. Cyberfile does not have a backup computer facility.	42. BCP
	43. Cyberfile does not have adequate alternative power sources.	43. BCP
	44. The DC does not have any building evacuation alarms to alert personnel and permit the orderly shutdown of operations and safe evacuation.	44. OPS
Conting. planning	45. A draft contingency plan did not have specific procedures to be followed in an emergency.	45. BCP
Risk analysis	46. The plan does not identify the key individuals responsible for executing specified procedures.	46. BCP
	47. The Cyberfile risk analysis was incomplete and did not adequately address physical, operational, and communication threats to the DC.	47. MGT
Security awareness	48. Cyberfile did not have a security awareness program.	48. MGT
	49. DC security practice was lax. A note was found written on a white board in the DC, instructing employees to hand off passwords to employees on the next shift.	49. MGT

Case #2: Montana Department of Administration data center audit results.

Audit category	Data center (DC) audit findings and recommendations	CBK domain
Planning and management	1. Maintain and update an inventory of systems in the data center.	1. MGT
	2. Coordinate with agencies with hosted systems to rank criticality and priority in which systems will be brought back up.	2. MGT
	3. Evaluate existing threats to the DC including the potential impact or harm.	3. MGT
	4. Conduct a cost analysis associated with implementing or improving controls.	4. MGT
	5. Define the responsibility for, and coordinate with agencies to utilize the existing software package to develop disaster recovery plans.	5. BCP
Physical security	6. Implement safeguards such as locked doors in building hallways and complete walls from suspended to real ceilings.	6. PHY
	7. Implement procedures and assign responsibilities for ensuring background checks are complete.	7. ACC
	8. Follow policy and maintain required authorization documentation on file for each individual who has key card access to the DC.	8. ACC
	9. Conduct a periodic review of all key card access to the DC to confirm appropriateness.	9. ACC

Appendix B (continued)

Audit category	Data center (DC) audit findings and recommendations	CBK domain
Environmental security	10. Monitor and review the key card activity logs and data center visitor logs for inappropriate or unauthorized access.	10. ACC
	11. Develop a system to ensure operator awareness of physical security breaches.	11. PHY
Recovery and incident response	12. Strengthen safeguards to mitigate the risks associated with earthquake and water-related threats.	12. PHY
	13. Maintain an updated statewide disaster recovery plan.	13. BCP
Why are security measures not given a priority?	14. Coordinate with the Governor's office to request that agencies assign a higher priority to disaster recovery.	14. BCP
	15. Clearly define and designate responsibility for coordination of all aspects of DC security.	15. MGT

Case #3: NYPD data center audit results.

Audit category	Data center (DC) audit findings	CBK domain
Computer system security	1. User accounts not adequately controlled by not deleting inactive accounts.	1. OPS
	2. Internet security plan was not reviewed or approved by proper authorities.	2. MGT
	3. Internet security controls such as firewalls and content filters, while installed, are not tested.	3. NET
Computer operations Backup tapes storage	4. Uninterruptable power supply systems were only capable of providing 12 min of backup power.	4. BCP
	5. NYPD should store backup tapes in a restricted and secure area.	5. BCP

Case #4: State of Michigan's Department of Information Technology.

Audit category	Data center (DC) audit recommendations	CBK domain
Risk assessments	1. DIT had not conducted a comprehensive risk assessment of hosting center operations or when systems, facilities, or other conditions changed.	1. MGT
	2. DIT had not established an effective process for developing and managing SLAs.	2. MGT
Service level agreements Strategic and operational planning	3. DIT had not developed a formal strategic plan and had not developed operational plans for its center activities.	3. OPS
	4. DIT had not developed formal cost-benefit analyses to determine hosting center alternatives, which would be helpful in identifying opportunities to improve operational efficiencies and associated risks.	4. MGT
Mainframe security	5. DIT had not fully implemented effective security practices for the Bull mainframe to include ensuring controls are functioning as intended.	5. ACC
Disaster recovery plan	6. DIT had not developed and tested disaster recovery plans for the hosting center facilities.	6. BCP
Policies and procedures	7. DIT had not updated or fully developed policies and procedures governing physical security and environmental controls at the hosting center.	7. PHY
Data exchange gateway security	8. DIT had not fully implemented security over the State's Data Exchange Gateway and thus could not ensure the gateway was protected from unauthorized access.	8. NET

References

- Chandler, C. (1996, September 29). The agency they love to get excited about — IRS's own problems and a complex tax code make it a favorite political target this year. *The Washington Post*, p. H1.
- Fisher, P. (2007). Operations security and controls. In H. F. Tipton, & M. Krause (Eds.), *Information Security Management Handbook* (pp. 2629–2639). (6th ed.). Boca Raton, FL: Taylor & Francis Group.

- GAO (1996). *GAO/AIMD-96-85R security weaknesses at IRS' Cyberfile data center*. Washington D. C: General Accounting Office, Accounting and Information Management Division.
- Hansche, S., Berti, J., & Hare, C. (2004). *Official (ISC)² guide to the CISSP exam*. New York: Auerbach.
- HHS (2008). Department of Health and Human Services' HIPAA security guidance. Retrieved March 27, 2008, from www.cms.hhs.gov
- Hoover, J. N. (2008, March 1). Data center best practices. *Information Week* 2010, from <http://www.informationweek.com/story/showArticle.jhtml?articleID=206900660>
- King, S. (2009). NYPD data center theft. Retrieved June 29, 2010, from http://www.computerweekly.com/blogs/stuart_king/2009/03/nypd-data-center.html
- Knapp, K. J., Ford, F. N., Marshall, T. E., & Rainer, K. R. J. (2007). The common body of knowledge: A framework to promote relevant information security research. *Journal of Digital Forensics, Security, and Law*, 2(1), 9–34.
- McTavish, T. H. (2007). *Audit report: Data center operations — State of Michigan, Department of Information Technology*. (No. 084-0580-06, Office of the Auditor General).
- Miller, R. (2010, 15 June). *Water main break floods Dallas Data Center (June 7, 2010)*. Data Center Knowledge www.datacenterknowledge.com
- Mitchell, R. L. (2009, July 28). Data centers go underground. *Computerworld* Retrieved July 2, 2010, from http://www.computerworld.com/s/article/9135735/Data_centers_go_underground
- Omaha World Herald (2010). 5 teams bid on NSA work [electronic version], April 24. Retrieved June 24, 2010, from <http://www.omaha.com/article/20100424/MONEY/704249845>
- Paquette, S., Jaeger, P. T., & Wilson, S. C. (2010). Identifying the security risks associated with governmental use of cloud computing. *Government Information Quarterly*, 27(3), 245–253.
- Privacy Rights Clearinghouse (2010). A chronology of data breaches. Retrieved June 24, 2010, from www.privacyrights.org
- Santos, O. (2007). *End-to-end network security: Defense-in-depth*. Indianapolis, IN: Cisco Press.
- Seacat, S. A. (2006). *Data center review, Department of Administration*. Helena, MT: Legislative Audit Division, State of Montana.
- Stout, D. (2007). *Memorandum. Re: Department of Administration, IS Audit Data Center Review Follow-up 07SP-025 (orig. 06DP-05)*. Helena, MT: Legislative Audit Division.
- Thibodeau, P. (2008, January 14). *Robbery alters thinking on data center security*. *Computer World* www.computerworld.com
- Thompson, W. C., Jr. (2006). *Audit report on the New York City Police Department data center*. New York: Office of the Comptroller, City of New York.
- Tipton, H. F. (Ed.). (2010). *Official (ISC)² guide to the CISSP CBK* (2nd ed.). Boca Raton, Florida: CRC Press — Taylor & Francis Group Boca Raton, Florida.
- Vijayan, J. (2004, June 28). ISO endorses key security certification. *ComputerWorld*, 38, 1–2.
- Wyld, D. (2009). *Moving to the cloud: An introduction to cloud computing in government*. IBM Center for the Business of Government.